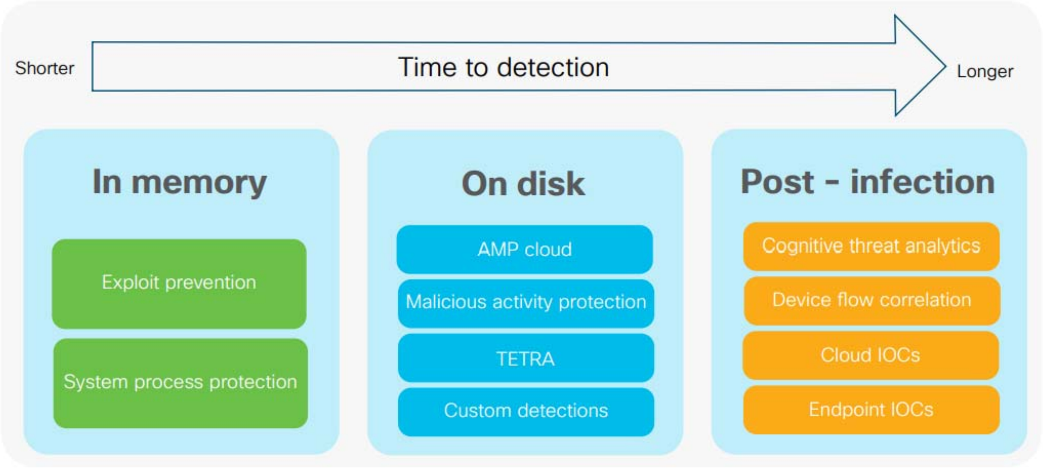
EXHIBIT 6

Patent No. 10,873,595, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
A method, comprising: at at least one server: identifying first vulnerability information utilizing second vulnerability information that is used to identify a plurality of potential vulnerabilities, the first vulnerability information being identified by:	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices *a method, comprising: at at least one server* (e.g., one or more servers that includes, accesses, and/or serves: the Cisco AMP for Endpoints/Connectors, global intelligence database/CVE database, AMP for Endpoints Console, etc.)*: identifying first vulnerability information* (e.g., a smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof, including associated information including but not limited to information describing the actual vulnerabilities themselves, information describing endpoints that contain the particular operating system/application/version thereof, information describing policy/detection/remediation techniques for addressing the actual vulnerabilities relevant to the particular operating system/application/version thereof including signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) *utilizing second vulnerability information* (e.g., a larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof, including associated information including but not limited to information describing the possible vulnerabilities themselves, information describing the different operating systems/applications/versions thereof, information describing policy/detection/remediation techniques for addressing the potential vulnerabilities relevant to the different operating systems/applications/versions thereof including signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) *that is used to identify a plurality of potential vulnerabilities* (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.)*, the first vulnerability information being identified by:* **<u>Note</u>**: See, for example, the evidence below (emphasis added, if any):

EXHIBIT 6

Claim 1 Elements	Applicability
	• "AMP Cloud provides access to the global intelligence database that is constantly updated and augmented with new detections and provides a great breadth of knowledge to the AMP Connector through one-to-one hash lookups, a generic signature engine, and the machine learning engine."  Shorter Time to detection Longer In memory Exploit prevention System process protection On disk AMP cloud Malicious activity protection TETRA Custom detections Post - infection Cognitive threat analytics Device flow correlation Cloud IOCs Endpoint IOCs https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.pdf "**Common Vulnerabilities and Exposures** The Common Vulnerabilities and Exposures (CVE) database records known vulnerabilities in various applications. All vulnerabilities are noted by their unique CVE ID. The CVE ID shown in the Console can be clicked to get more details on the vulnerability."

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
Cisco <i>AMP for Endpoints User Guide</i>, Chapter 20, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020

“Designed for Cisco Firepower® network threat appliances, AMP for Networks detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.” https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)

“<b>Features and Benefits of Cisco AMP for Endpoints</b>”

<table>
<tr><th>Feature</th><th>Benefits</th></tr>
<tr><td>. . .</td><td>. . .</td></tr>
<tr><td>Dashboards</td><td>Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a comprehensive contextual view so that you can make informed security decisions.</td></tr>
<tr><td>. . .</td><td>. . .</td></tr>
<tr><td>Exploit Prevention</td><td>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes. The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>payload, and zero-day attacks on software vulnerabilities yet to be patched.</td></tr>
<tr><td>. . .</td><td>. . .</td></tr>
<tr><td>Vulnerabilities</td><td>Identify vulnerable software and close attack pathways. This feature shows a list of hosts that contain vulnerable software, a list of the vulnerable software on each host, and the hosts most likely to be compromised. Powered by our threat intelligence and security analytics, AMP identifies vulnerable software being targeted by malware, shows you the potential exploit, and provides you with a prioritized list of hosts to patch.</td></tr>
</table>
https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)
</td></tr>
<tr><td>identifying at least one operating system of a plurality of devices, and</td><td>
Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for <i>identifying at least one operating system</i> (e.g., a Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) <i>of a plurality of devices</i> (e.g., 50+ nodes licensed to use the software, etc.)<i>, and</i>

<b>Note</b>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

<b>Note</b>: Each node has “AMP for Endpoint” Connector software installed thereon that identifies the operating system/applications/versions thereof on such node.

<b>“Deployment Options for Protection Everywhere</b>
</td></tr>
</table>

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, the AMP solution can be deployed at different control points throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:”
<table>
<tr><th>Product Name</th><th>Details</th></tr>
<tr><td>Cisco AMP for Endpoints</td><td>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.</td></tr>
</table>
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)

“<b>Software requirements</b>”
<table>
<tr><td>Cisco AMP for Endpoints</td><td>● Microsoft Windows XP with Service Pack 3 or later
● Microsoft Windows Vista with Service Pack 2 or later
● Microsoft Windows 7
● Microsoft Windows 8 and 8.1
● Microsoft Windows 10
● Microsoft Windows Server 2003
● Microsoft Windows Server 2008
● Microsoft Windows Server 2012
● Mac OS X 10.7 and later
● Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3
● Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Cisco AMP for Endpoints on Android mobile devices</td><td>Android version 2.1 and later</td></tr>
<tr><td>Cisco AMP for Endpoints on Apple iOS</td><td>MDM supervised iOS version 11</td></tr>
</table>
https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html

“Cisco’s AMP for endpoints subscription offerings begin with a minimum of 50 nodes, and thus inherently the network would include a plurality of devices (e.g., nodes, etc.), that include at least a first, second, and third device.”
http://winncom.com.ua/wp-content/uploads/2018/06/Cisco-Advanced-Malware-Protection-for-Endpoints.pdf</td></tr>
<tr><td>based on the at least one operating system, identifying at least one of the plurality of potential vulnerabilities as an actual vulnerability of a plurality of actual vulnerabilities of the at least one operating system to which the plurality of devices is actually vulnerable; and</td><td>Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for, *based on the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.), *identifying at least one of the plurality of potential vulnerabilities* (e.g., the possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.) *as an actual vulnerability of a plurality of actual vulnerabilities* (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *to which the plurality of devices* (e.g., the 50+ nodes licensed to use the software, etc.) *is actually vulnerable; and*</td></tr>
</table>

Claim 1 Elements	Applicability
	<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **<u>Note</u>**: Each node has "AMP for Endpoint" Connector software installed thereon that identifies the operating system/applications/versions thereof on such node and, based thereon, uses the second vulnerability information (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) to identify the first vulnerability information (e.g., the smaller "sub-set" of actual vulnerabilities relevant to the particular operating system/applications/versions thereof on the particular node). "Whenever an executable file is moved, copied, or executed the AMP for Endpoints Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database that information is displayed on the Vulnerable Software page. Currently the following applications and versions on Windows operating systems are reported on the vulnerabilities page: ... By default, all known vulnerable programs are shown. ... Additional information is available at the bottom of the expanded program list item. The following topics provide additional information through the associated links: • Observed in Groups • Last Observed (computer)

Claim 1 Elements	Applicability
	• Events • File Trajectory" Cisco *AMP for Endpoints User Guide*, Chapter 20, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
communicating, from the at least one server and to at least one of the plurality of devices over at least one network, the first vulnerability information, the first vulnerability information corresponding with the actual vulnerabilities of the at least one operating system of the at least one device, and excluding at least a portion of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for *communicating, from the at least one server* (e.g., the one or more servers that includes, accesses, and/or serves: the Cisco AMP for Endpoints/Connectors, global intelligence database/CVE database, AMP for Endpoints Console, etc.) *and to at least one of the plurality of devices* (e.g., one of the 50+ nodes licensed to use the software, etc.) *over at least one network, the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof)*, the first vulnerability information corresponding with the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *of the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*, and excluding at least a portion of the second vulnerability information* (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) *that does not correspond with the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *of the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*;* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

Claim 1 Elements	Applicability
	Note: As set forth below, Cisco AMP for Endpoints includes AMP Update Server software that generates (and communicates to the Connectors/devices) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software) utilizing the second vulnerability information (e.g., ALL signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software available at the AMP Update server and/or other update servers). As set forth below, the AMP Update Server and/or other servers automatically determine which of the updates to generate and communicate. **Note**: As set forth below, a subset of virus scanner updates (e.g., TETRA signatures, etc.) are communicated to the Connectors. "The AMP Update Server is designed to reduce the high volume of network traffic consumed by the AMP for Endpoints Windows Connector while fetching TETRA definition updates from Cisco servers. The utility aims to reduce the update bandwidth consumption by acting either as a caching HTTP proxy server, or by periodically fetching updates to a location that can be served by an on-premises HTTP server that you must set up and configure. You must enable your Local AMP Update Server under the TETRA section of your Windows policies. It may take an hour or longer for the AMP Update Server to download initial content from the Cisco Cloud." Cisco *AMP for Endpoints User Guide*, Chapter 27, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 **Note**: As set forth below, a subset of intrusion-related updates (e.g., Exploit Prevention Engine information, etc.) are communicated to the Connectors.

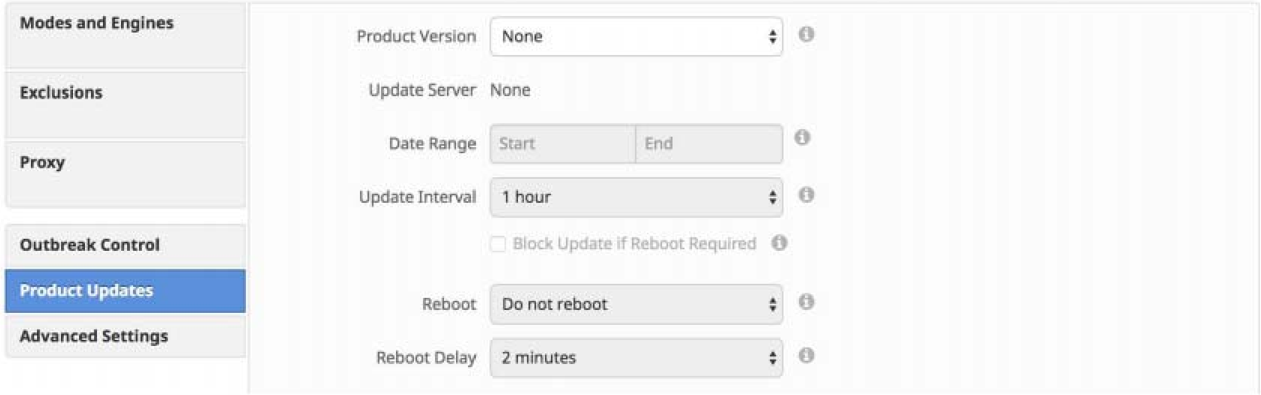
Claim 1 Elements	Applicability
	"Updated Exploit Prevention Engine to include changes related to the vulnerability described in CVE-2020-0796." Cisco *AMP for Endpoints Release Notes*, June 25, 2020 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) "**AMP for Endpoints Console 5.4.20200624** Bugfixes/Updates • Fixed issue where MSSP partners were not able to see more than 25 customers on the MSSP partner page. (CSCvu61075) • Updated list of processes protected by and excluded from the AMP for Endpoints Windows Exploit Prevention engine." Cisco *AMP for Endpoints Release Notes*, June 24, 2020 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) "AMP for Endpoints Premier subscriptions include Cisco SecureX Threat Hunting. Cisco SecureX Threat Hunting leverages the expertise of both Talos and the Cisco AMP Efficacy Research Team to help identify threats found within the customer environment. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. Once threats are detected, customers are notified so they can begin remediation. ... **Remediation** includes recommendations on actions that can or should be taken, to include pointed investigation components from the incident. Any possible mitigation measures for the specific incident may be included if applicable."

Claim 1 Elements	Applicability
	Cisco *AMP for Endpoints User Guide*, Chapter 28, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 “**Exploit Prevention** (Connector version 6.0.5 and later) The AMP for Endpoints Exploit Prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine. You can use Device Trajectory to help determine the vector of the attack and add it to a **Custom Detections - Simple** list. To enable the exploit prevention engine, go to Modes and Engines in your policy and select Audit or Block mode. Audit mode is only available on AMP for Endpoints Windows Connector 7.3.1 and later. Earlier versions of the Connector will treat Audit mode the same as Block mode.” Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "AMP for Endpoints Exploit Prevention ...- Device Flow Correlation, which inspects incoming and outgoing network communications of a process/file on the endpoint and allows the enforcement of a restrictive action according to the policy." Page 13, (https://www.cisco.com/c/dam/en/us/products/collateral/security/mitre-att-ck-wp.pdf Last Updated: April 2020 **Note**: As set forth below, a subset of firewall updates (e.g., firewall-related isolation information, etc.) are communicated to the Connectors.

Claim 1 Elements	Applicability
	“**AMP for Endpoints Console 5.4.20191001** New • Beta - Endpoint Isolation IP Allow lists: there is a new Endpoint Isolation IP Allow list type under Outbreak Control > Network - IP Block & Allow Lists. • IP lists with no ports and less than 200 IP addresses that are connected to Endpoint Isolation in policies will be migrated; IP lists that don’t meet these criteria will not be migrated and will need to be recreated as Endpoint Isolation IP Allow lists and added to the Endpoint Isolation policy. • Policies and groups using the Endpoint Isolation IP Allow lists will appear in the IP List details panel. All new IP allow lists for Endpoint Isolation must be created using this new list type.” Cisco *AMP for Endpoints Release Notes*, October 1, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) “**AMP for Endpoints Windows Connector 7.0.5** New • Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. • System Process Protection notifications • are less verbose. (CSCvn41948) • are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)” Cisco *AMP for Endpoints Release Notes*, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)

Claim 1 Elements	Applicability
	"**Blocked List Data Source** enables you to select the IP blocked lists your Connectors use. If you select Custom, your Connectors will only use the IP blocked lists you have added to the policy. Choose Cisco to have your Connectors only use the Cisco Intelligence Feed to define malicious sites. The Cisco Intelligence Feed represents IP addresses determined by Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If Talos continues to observe poor behavior related to an address it will be added back to the list. The Custom and Cisco option will allow you to use both the IP blocked lists you have added to the policy and the Cisco Intelligence Feed." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 **Note**: Following is evidence of other update servers (other than the AMP Update Server): "**North America Firewall Exceptions** Organizations located in North America must allow connectivity from the Connector to the following servers over HTTPS (TCP 443): • Event Server - intake.amp.cisco.com • Management Server - mgmt.amp.cisco.com • Policy Server - policy.amp.cisco.com • Error Reporting - crash.amp.cisco.com • Endpoint IOC Downloads - ioc.amp.cisco.com • Advanced Custom Signatures - custom-signatures.amp.cisco.com • Connector Upgrades - upgrades.amp.cisco.com (TCP 80 and 443) • Remote File Fetch - rff.amp.cisco.com

Claim 1 Elements	Applicability
	To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443: • Cloud Host - cloud-ec.amp.cisco.com For AMP for Endpoints Windows version 5.0 and higher you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead: • Cloud Host - cloud-ec-asn.amp.cisco.com • Enrollment Server - enrolment.amp.cisco.com If you have TETRA enabled on any of your AMP for Endpoints Connectors you must allow access to the following server over TCP 80 and 443 for signature updates: • Update Server - tetra-defs.amp.cisco.com To use Orbital on your AMP for Endpoints Connectors, you must allow access to the following servers over TCP 443: • Orbital Updates - orbital.amp.cisco.com • Orbital Queries - ncp.orbital.amp.cisco.com • Orbital Installer - update.orbital.amp.cisco.com If you have Behavioral Protection enabled on your AMP for Endpoints Windows Connectors you need to allow access to the following server over TCP 443 for signature updates: • Behavioral Protection Signatures - apde.amp.cisco.com" Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**Cisco-Maintained Exclusions** Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus, security, or other software. Click the Cisco-Maintained Exclusions button to view the list of exclusions. These cannot be deleted or

Claim 1 Elements	Applicability
	modified and are presented so you can see which files and directories are being excluded for each application. These exclusions may also be updated over time with improvements and new exclusions may be added for new versions of an application. When one of these exclusions is updated, any policies using the exclusion will also be updated so the new exclusions are pushed to your Connectors. Each row displays the operating system, exclusion set name, the number of exclusions, the number of groups using the exclusion set, and the number of computers using the exclusion set. You can use the search bar to find exclusion sets by name, path, extension, threat name, or SHA-256. You can also filter the list by operating system by clicking on the respective tabs.” Cisco *AMP for Endpoints User Guide*, Chapter 3, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 “**Windows Connector: Product Updates**  Modes and Engines Exclusions Proxy Outbreak Control Product Updates Advanced Settings Product Version: None Update Server: None Date Range: Start End Update Interval: 1 hour □ Block Update if Reboot Required Reboot: Do not reboot Reboot Delay: 2 minutes

Claim 1 Elements	Applicability
	When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the **Product Version** dropdown menu showing which version you are going to and it will populate the **Update Server** so you can see where the files will be pulled from. There will also be information to show how many Connectors in groups that use the policy will require a reboot after updating. You can then define the window in which updates are allowed to occur by choosing a **Date Range**. In **Date Range**, click **Start** to select a date and time for your start window and **End** to select a date and time for your end window. The **Update Interval** allows you to specify how long your Connectors will wait between checks for new product updates, including Orbital updates. This can be configured between every 30 minutes to every 24 hours to reduce network traffic. Between the times set in the **Date Range**, if a Connector calls home to pick up a policy, it will pick up the product update. Because the Connector calls home at an interval dependent on the Heartbeat Interval, you will want to plan your Update Window accordingly; that is, make sure the interval specified in the Update Window is larger than the Heartbeat Interval. If you are updating to version 4.3 or later of the AMP for Endpoints Windows Connector you will be presented with different reboot options. As of version 4.3 some updates may not require a reboot to take effect." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
at the at least one device:	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for, *at the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*:* *receiving, from the at least one server* (e.g., the one or more servers that includes, accesses,

Claim 1 Elements	Applicability
receiving, from the at least one server over the at least one network, the first vulnerability information;	and/or serves: the Cisco AMP for Endpoints/Connectors, global intelligence database/CVE database, AMP for Endpoints Console, etc.) *over the at least one network, the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof)*;* **<u>Note</u>**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **<u>Note</u>**: As set forth below, Cisco AMP for Endpoints includes AMP Update Server software that generates (and communicates to the Connectors/devices) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software) utilizing the second vulnerability information (e.g., ALL signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software available at the AMP Update server and/or other update servers). As set forth below, the AMP Update Server and/or other servers automatically determine which of the updates to generate and communicate, for each device to receive. **<u>Note</u>**: As set forth below, a subset of virus scanner updates (e.g., TETRA signatures, etc.) are communicated to the Connectors. "The AMP Update Server is designed to reduce the high volume of network traffic consumed by the AMP for Endpoints Windows Connector while <u>fetching TETRA definition updates from Cisco servers</u>. The utility aims to reduce the update bandwidth consumption by acting either as a caching HTTP proxy server, or by periodically fetching updates to a location that can be served by an on-premises HTTP server that you must set up and configure. You must enable your Local AMP Update Server under the TETRA section of your Windows policies. It may take an hour or longer for the AMP Update Server to download initial content from the Cisco Cloud."

Claim 1 Elements	Applicability
	Cisco *AMP for Endpoints User Guide*, Chapter 27, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 **Note**: As set forth below, a subset of intrusion-related updates (e.g., Exploit Prevention Engine information, etc.) are communicated to the Connectors. "**AMP for Endpoints Console 5.4.20200624** Bugfixes/Updates • Fixed issue where MSSP partners were not able to see more than 25 customers on the MSSP partner page. (CSCvu61075) • Updated list of processes protected by and excluded from the AMP for Endpoints Windows Exploit Prevention engine." Cisco *AMP for Endpoints Release Notes*, June 24, 2020 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) "AMP for Endpoints Premier subscriptions include Cisco SecureX Threat Hunting. Cisco SecureX Threat Hunting leverages the expertise of both Talos and the Cisco AMP Efficacy Research Team to help identify threats found within the customer environment. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. Once threats are detected, customers are notified so they can begin remediation. ... **Remediation** includes recommendations on actions that can or should be taken, to include pointed investigation components from the incident. Any possible mitigation measures for the specific incident may be included if applicable."

Claim 1 Elements	Applicability
	Cisco *AMP for Endpoints User Guide*, Chapter 28, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 “**Exploit Prevention** (Connector version 6.0.5 and later) The AMP for Endpoints Exploit Prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine. You can use Device Trajectory to help determine the vector of the attack and add it to a **Custom Detections - Simple** list. To enable the exploit prevention engine, go to Modes and Engines in your policy and select Audit or Block mode. Audit mode is only available on AMP for Endpoints Windows Connector 7.3.1 and later. Earlier versions of the Connector will treat Audit mode the same as Block mode.” Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "AMP for Endpoints Exploit Prevention ...- Device Flow Correlation, which inspects incoming and outgoing network communications of a process/file on the endpoint and allows the enforcement of a restrictive action according to the policy." Page 13, (https://www.cisco.com/c/dam/en/us/products/collateral/security/mitre-att-ck-wp.pdf Last Updated: April 2020 **<u>Note</u>**: As set forth below, a subset of firewall updates (e.g., firewall-related isolation information, etc.) are communicated to the Connectors.

Claim 1 Elements	Applicability
	“**AMP for Endpoints Console 5.4.20191001** New • Beta - Endpoint Isolation IP Allow lists: there is a new Endpoint Isolation IP Allow list type under Outbreak Control > Network - IP Block & Allow Lists. • IP lists with no ports and less than 200 IP addresses that are connected to Endpoint Isolation in policies will be migrated; IP lists that don’t meet these criteria will not be migrated and will need to be recreated as Endpoint Isolation IP Allow lists and added to the Endpoint Isolation policy. • Policies and groups using the Endpoint Isolation IP Allow lists will appear in the IP List details panel. All new IP allow lists for Endpoint Isolation must be created using this new list type.” Cisco *AMP for Endpoints Release Notes*, October 1, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) “**AMP for Endpoints Windows Connector 7.0.5** New • Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. • System Process Protection notifications • are less verbose. (CSCvn41948) • are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)” Cisco *AMP for Endpoints Release Notes*, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)

Claim 1 Elements	Applicability
	"Blocked List Data Source enables you to select the IP blocked lists your Connectors use. If you select Custom, your Connectors will only use the IP blocked lists you have added to the policy. Choose Cisco to have your Connectors only use the Cisco Intelligence Feed to define malicious sites. The Cisco Intelligence Feed represents IP addresses determined by Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If Talos continues to observe poor behavior related to an address it will be added back to the list. The Custom and Cisco option will allow you to use both the IP blocked lists you have added to the policy and the Cisco Intelligence Feed." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
identifying a first portion of the first vulnerability information that includes data inspection-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device, and that excludes other data inspection-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for *identifying a first portion of the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof,) *that includes data inspection-related information* (e.g., signature/policy updates for anti-virus software, etc.) *that corresponds with at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *of the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*, and that excludes other data inspection-related information of the second vulnerability information* (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) *that does not correspond with the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an

Claim 1 Elements	Applicability
at least one operating system of the at least one device;	application/version thereof, etc.) *of the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*;* **<u>Note</u>**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **<u>Note</u>**: As set forth below, a subset of virus scanner updates (e.g., TETRA signatures, etc.) are communicated to the Connectors. "The AMP Update Server is designed to reduce the high volume of network traffic consumed by the AMP for Endpoints Windows Connector while <u>fetching TETRA definition updates from Cisco servers</u>. The utility aims to reduce the update bandwidth consumption by acting either as a caching HTTP proxy server, or by periodically fetching updates to a location that can be served by an on-premises HTTP server that you must set up and configure. You must enable your Local AMP Update Server under the TETRA section of your Windows policies. It may take an hour or longer for the AMP Update Server to download initial content from the Cisco Cloud." Cisco *AMP for Endpoints User Guide*, Chapter 27, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
identifying a first event of a plurality of events in connection with the at least one device; causing a determination that the at least one of the actual vulnerabilities corresponding	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for *identifying a first event of a plurality of events* (e.g., a first discrete event that triggers at least one of the signature/policy updates for the anti-virus software, etc.) *in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*; causing a determination that the at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the data inspection-related information* (e.g., the signature/policy updates for anti-virus

Claim 1 Elements	Applicability
with the data inspection-related information is susceptible to being taken advantage of by the first event identified in connection with the at least one device, utilizing the data inspection-related information; identifying a second event of the plurality of events in connection with the at least one device; causing a determination that the at least one of the actual vulnerabilities corresponding with the data inspection-related information is not susceptible to being taken advantage of by the second event identified in connection with the at least one device, utilizing the data inspection-related information;	software, etc.) *is susceptible to being taken advantage of by the first event identified in connection with the at least one device*(e.g., one of the 50+ nodes licensed to use the software, etc.), *utilizing the data inspection-related information* (e.g., the signature/policy updates for anti-virus software, etc.)*; identifying a second event of the plurality of events* (e.g., a second discrete event that does <u>not</u> trigger any of the signature/policy updates for the anti-virus software, etc.) *in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*; causing a determination that the at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the data inspection-related information* (e.g., the signature/policy updates for anti-virus software, etc.) *is not susceptible to being taken advantage of by the second event* (e.g., a second discrete event that does <u>not</u> trigger any of the signature/policy updates for the anti-virus software, etc.) *identified in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*, utilizing the data inspection-related information* (e.g., the signature/policy updates for anti-virus software, etc.)*;* **<u>Note</u>**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **<u>Note</u>**: The TETRA/ClamAV anti-virus software includes signatures/policies that are triggered by some events (e.g., the first event, etc.), and that are not triggered by other events (e.g., the second event, etc.), so that only malicious events (relevant to the device's operating system) trigger a response. "**TETRA**

Claim 1 Elements	Applicability
	TETRA is a full antivirus replacement and should never be enabled if another antivirus engine is installed. TETRA can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a large environment. To enable TETRA and adjust settings go to **Advanced Settings > TETRA** in your policy." Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**Detection Engines** Windows, Mac, and Linux Connectors have the option of enabling offline detection engines (**TETRA** for Windows and **ClamAV** for Mac and Linux) to protect the endpoint from malware without connecting to the Cisco Cloud to query each file." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
identifying a second portion of the first vulnerability information that includes traffic inspection-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device, and that excludes other	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for *identifying a second portion of the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof,) *that includes traffic inspection-related information* (e.g., signature/policy updates for intrusion-detection software, etc.) *that corresponds with at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *of the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*, and that excludes other traffic*

Claim 1 Elements	Applicability
traffic inspection-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;	*inspection-related information of the second vulnerability information* (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) *that does not correspond with the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g.*,* the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *of the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*;* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: As set forth below, a subset of intrusion-related updates (e.g., Exploit Prevention Engine information, etc.) are communicated to the Connectors. "Updated Exploit Prevention Engine to include changes related to the vulnerability described in CVE-2020-0796." Cisco *AMP for Endpoints Release Notes*, June 25, 2020 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) "**AMP for Endpoints Console 5.4.20200624** Bugfixes/Updates • Fixed issue where MSSP partners were not able to see more than 25 customers on the MSSP partner page. (CSCvu61075) • Updated list of processes protected by and excluded from the AMP for Endpoints Windows Exploit Prevention engine."

Claim 1 Elements	Applicability
	Cisco *AMP for Endpoints Release Notes*, June 24, 2020 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)
identifying a third event of the plurality of events in connection with the at least one device; causing a determination that the at least one of the actual vulnerabilities corresponding with the traffic inspection-related information is susceptible to being taken advantage of by the third event identified in connection with the at least one device, utilizing the traffic inspection-related information; identifying a fourth event of the plurality of events in connection with the at least one device; causing a determination that the at least one of the actual vulnerabilities corresponding with the traffic inspection-	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for *identifying a third event of the plurality of events* (e.g., a third discrete event that triggers at least one of the signature/policy updates for the intrusion detection software, etc.) *in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*; causing a determination that the at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the traffic inspection-related information* (e.g., signature/policy updates for intrusion detection software, etc.) *is susceptible to being taken advantage of by the third event* (e.g., a third discrete event that triggers at least one of the signature/policy updates for the intrusion detection software, etc.) *identified in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*, utilizing the traffic inspection-related information* (e.g., signature/policy updates for intrusion detection software, etc.)*; identifying a fourth event of the plurality of events* (e.g., a fourth discrete event that does not trigger at least one of the signature/policy updates for the intrusion detection software, etc.) *in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*; causing a determination that the at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the traffic inspection-related information* (e.g., signature/policy updates for intrusion detection software, etc.) *is not susceptible to being taken advantage of by the fourth event* (e.g., a fourth discrete event that does not trigger at least one of the signature/policy updates for the intrusion detection software, etc.) *identified in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*, utilizing the traffic inspection-related information* (e.g., signature/policy updates for intrusion detection software, etc.)*;*

Claim 1 Elements	Applicability
related information is not susceptible to being taken advantage of by the fourth event identified in connection with the at least one device, utilizing the traffic inspection-related information;	**Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: The anti-intrusion software includes signatures/policies that are triggered by some events (e.g., the third event, etc.), and that are not triggered by other events (e.g., the fourth event, etc.), so that only malicious events (relevant to the device's operating system) trigger a response. "**Detect and Block Exploit Attempts** Cisco AMP for Networks builds on the Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS). When the system is deployed in line, it detects and blocks client-side exploit attempts that can lead to malicious file downloads, commonly referred to as drive-by attacks. The NGIPS system can also protect against other vulnerability exploit attempts aimed at web browsers, Adobe Acrobat, Java, Flash, and other commonly targeted client applications. Acting as early as possible in the attack chain, the system attempts to limit collateral damage and avoid costly cleanup efforts." https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added) "**Exploit Prevention** (Connector version 6.0.5 and later) The AMP for Endpoints Exploit Prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine. You can use Device Trajectory to help determine the vector of the attack and add it to a **Custom Detections - Simple** list.

Claim 1 Elements	Applicability
	To enable the exploit prevention engine, go to Modes and Engines in your policy and select Audit or Block mode. Audit mode is only available on AMP for Endpoints Windows Connector 7.3.1 and later. Earlier versions of the Connector will treat Audit mode the same as Block mode." Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "AMP for Endpoints Premier subscriptions include Cisco SecureX Threat Hunting. Cisco SecureX Threat Hunting leverages the expertise of both Talos and the Cisco AMP Efficacy Research Team to help identify threats found within the customer environment. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. Once threats are detected, customers are notified so they can begin remediation. ... **Remediation** includes recommendations on actions that can or should be taken, to include pointed investigation components from the incident. Any possible mitigation measures for the specific incident may be included if applicable." Cisco *AMP for Endpoints User Guide*, Chapter 28, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**AMP for Endpoints Exploit Prevention** ...- Device Flow Correlation, which inspects incoming and outgoing network communications of a process/file on the endpoint and allows the enforcement of a restrictive action according to the policy." Page 13, (https://www.cisco.com/c/dam/en/us/products/collateral/security/mitre-att-ck-wp.pdf) Last Updated: April 2020

Claim 1 Elements	Applicability
identifying a third portion of the first vulnerability information that includes firewall-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device, and that excludes other firewall-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for *identifying a third portion of the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof) *that includes firewall-related information* (e.g., signature/policy updates for firewall software, etc.) *that corresponds with at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *of the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.), *and that excludes other firewall-related information of the second vulnerability information* (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) *that does not correspond with the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *of the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*;* **<u>Note</u>**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **<u>Note</u>**: As set forth below, a subset of firewall updates (e.g., firewall-related isolation information, etc.) are communicated to the Connectors. "**AMP for Endpoints Console 5.4.20191001** New • Beta - Endpoint Isolation IP Allow lists: there is a new Endpoint Isolation IP Allow list type under Outbreak Control > Network - IP Block & Allow Lists.

Claim 1 Elements	Applicability
	• IP lists with no ports and less than 200 IP addresses that are connected to Endpoint Isolation in policies will be migrated; IP lists that don't meet these criteria will not be migrated and will need to be recreated as Endpoint Isolation IP Allow lists and added to the Endpoint Isolation policy. • Policies and groups using the Endpoint Isolation IP Allow lists will appear in the IP List details panel. All new IP allow lists for Endpoint Isolation must be created using this new list type." Cisco *AMP for Endpoints Release Notes*, October 1, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) "**AMP for Endpoints Windows Connector 7.0.5** New • Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. • System Process Protection notifications • are less verbose. (CSCvn41948) • are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)" Cisco *AMP for Endpoints Release Notes*, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf) "**Blocked List Data Source** enables you to select the IP blocked lists your Connectors use. If you select Custom, your Connectors will only use the IP blocked lists you have added to the policy. Choose Cisco to have your Connectors only use the Cisco Intelligence Feed to define malicious sites. The Cisco Intelligence Feed represents IP addresses determined by Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If Talos continues to

Claim 1 Elements	Applicability
	observe poor behavior related to an address it will be added back to the list. The Custom and Cisco option will allow you to use both the IP blocked lists you have added to the policy and the Cisco Intelligence Feed.” Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 **Note**: Following is evidence of other update servers (other than the AMP Update Server): “**North America Firewall Exceptions** Organizations located in North America must allow connectivity from the Connector to the following servers over HTTPS (TCP 443): • Event Server - intake.amp.cisco.com • Management Server - mgmt.amp.cisco.com • Policy Server - policy.amp.cisco.com • Error Reporting - crash.amp.cisco.com • Endpoint IOC Downloads - ioc.amp.cisco.com • Advanced Custom Signatures - custom-signatures.amp.cisco.com • Connector Upgrades - upgrades.amp.cisco.com (TCP 80 and 443) • Remote File Fetch - rff.amp.cisco.com To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443: • Cloud Host - cloud-ec.amp.cisco.com For AMP for Endpoints Windows version 5.0 and higher you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead: • Cloud Host - cloud-ec-asn.amp.cisco.com

Patent No. 10,873,595, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

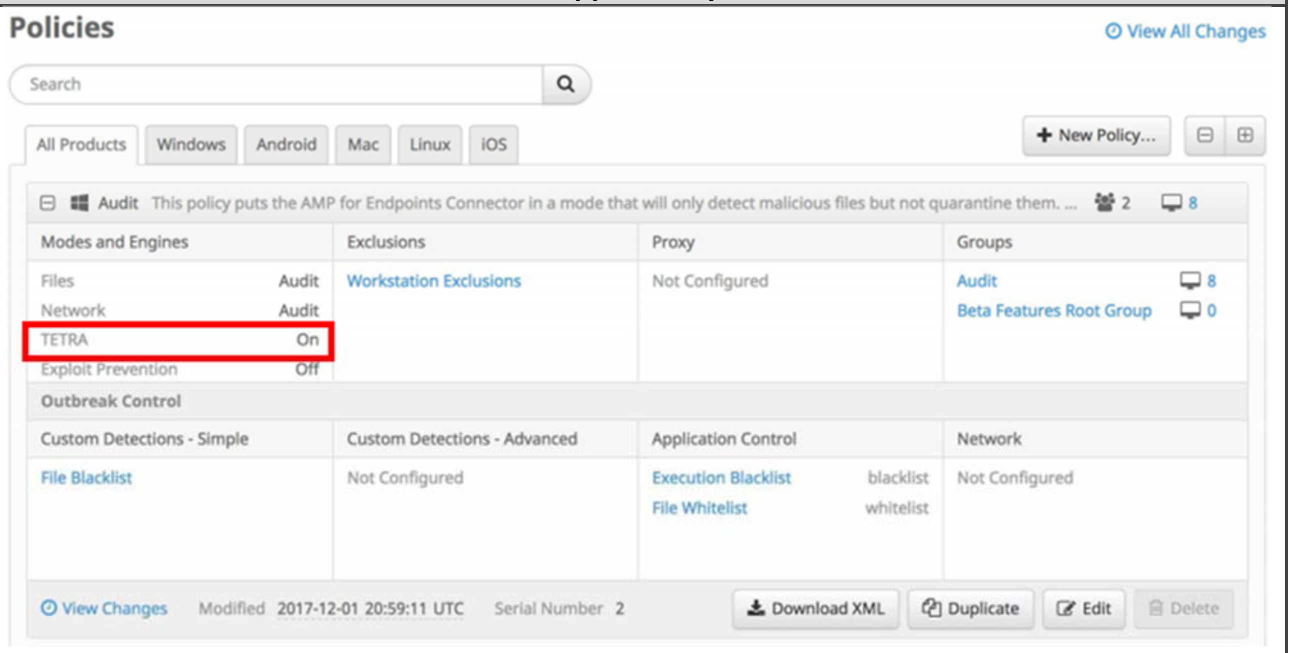
Claim 1 Elements	Applicability
	• Enrollment Server - enrolment.amp.cisco.com If you have TETRA enabled on any of your AMP for Endpoints Connectors you must allow access to the following server over TCP 80 and 443 for signature updates: • Update Server - tetra-defs.amp.cisco.com To use Orbital on your AMP for Endpoints Connectors, you must allow access to the following servers over TCP 443: • Orbital Updates - orbital.amp.cisco.com • Orbital Queries - ncp.orbital.amp.cisco.com • Orbital Installer - update.orbital.amp.cisco.com If you have Behavioral Protection enabled on your AMP for Endpoints Windows Connectors you need to allow access to the following server over TCP 443 for signature updates: • Behavioral Protection Signatures - apde.amp.cisco.com" Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**Cisco-Maintained Exclusions** Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus, security, or other software. Click the Cisco-Maintained Exclusions button to view the list of exclusions. These cannot be deleted or modified and are presented so you can see which files and directories are being excluded for each application. These exclusions may also be updated over time with improvements and new exclusions may be added for new versions of an application. When one of these exclusions is updated, any policies using the exclusion will also be updated so the new exclusions are pushed to your Connectors.

Claim 1 Elements	Applicability
	Each row displays the operating system, exclusion set name, the number of exclusions, the number of groups using the exclusion set, and the number of computers using the exclusion set. You can use the search bar to find exclusion sets by name, path, extension, threat name, or SHA-256. You can also filter the list by operating system by clicking on the respective tabs." Cisco *AMP for Endpoints User Guide*, Chapter 3, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
identifying a fifth event of the plurality of events in connection with the at least one device; causing a determination that the at least one of the actual vulnerabilities corresponding with the firewall-related information is susceptible to being taken advantage of by the fifth event identified in connection with the at least one device, utilizing the firewall-related information; identifying a sixth event of the plurality of events in connection with the at least one device; and	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for *identifying a fifth event of the plurality of events* (e.g., a fifth discrete event that triggers at least one of the signature/policy updates for the firewall software, etc.) *in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*; causing a determination that the at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the firewall-related information* (e.g., signature/policy updates for firewall software, etc.) *is susceptible to being taken advantage of by the fifth event* (e.g., a fifth discrete event that triggers at least one of the signature/policy updates for the firewall software, etc.) *identified in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.), *utilizing the firewall-related information* (e.g., signature/policy updates for firewall software, etc.)*; identifying a sixth event of the plurality of events* (e.g., a sixth discrete event that does <u>not</u> trigger at least one of the signature/policy updates for the firewall software, etc.) *in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*; and causing a determination that the at least one of the actual vulnerabilities* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *corresponding with the firewall-related information* (e.g., signature/policy updates for firewall software, etc.) *is not susceptible to being taken advantage of by the sixth event* (e.g., a sixth discrete event that does <u>not</u> trigger at least one of the signature/policy updates for the

Claim 1 Elements	Applicability
causing a determination that the at least one of the actual vulnerabilities corresponding with the firewall-related information is not susceptible to being taken advantage of by the sixth event identified in connection with the at least one device, utilizing the firewall-related information; and	firewall software, etc.) *identified in connection with the at least one device* (e.g., one of the 50+ nodes licensed to use the software, etc.)*, utilizing the firewall-related information* (e.g., signature/policy updates for firewall software, etc.)*;* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: The firewall software includes signatures/policies that are triggered by some events (e.g., the fifth event, etc.), and that are not triggered by other events (e.g., the sixth event, etc.), so that only malicious events (relevant to the device's operating system) trigger a response. "**Firewall Connectivity** To allow the AMP for Endpoints Connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are three sets of servers depending on where you are located: one for the European Union, one for Asia Pacific, Japan, and Greater China, and one for the rest of the world. IMPORTANT! If your firewall requires IP address exceptions, see this Cisco TechNote." Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**AMP for Endpoints Windows Connector 7.0.5** New

Claim 1 Elements	Applicability
	• Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. • System Process Protection notifications • are less verbose. (CSCvn41948) • are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)" Cisco *AMP for Endpoints Release Notes*, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)
at at least one administrator computer: in response to administrator action, causing setting, before the first and second events, of a first policy associated with utilizing the data inspection-related information that is applied to a group including each of the plurality of devices that has the at least one operating system;	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for, *at at least one administrator computer* (e.g., a machine with a browser for accessing the AMP for Endpoints Console, etc.)*: in response to administrator action* (e.g., user input, etc.)*, causing setting, before the first and second events, of a first policy* (e.g., a policy for anti-virus software, etc.) *associated with utilizing the data inspection-related information* (e.g., signature/policy updates for anti-virus software, etc.) *that is applied to a group including each of the plurality of devices* (e.g., the 50+ nodes licensed to use the software, etc.) *that has the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.)*;* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "**System Requirements** To access the AMP for Endpoints Console, you will need one of the following Web browsers: • Internet Explorer 11 or higher • Microsoft Edge 38.14393 or higher

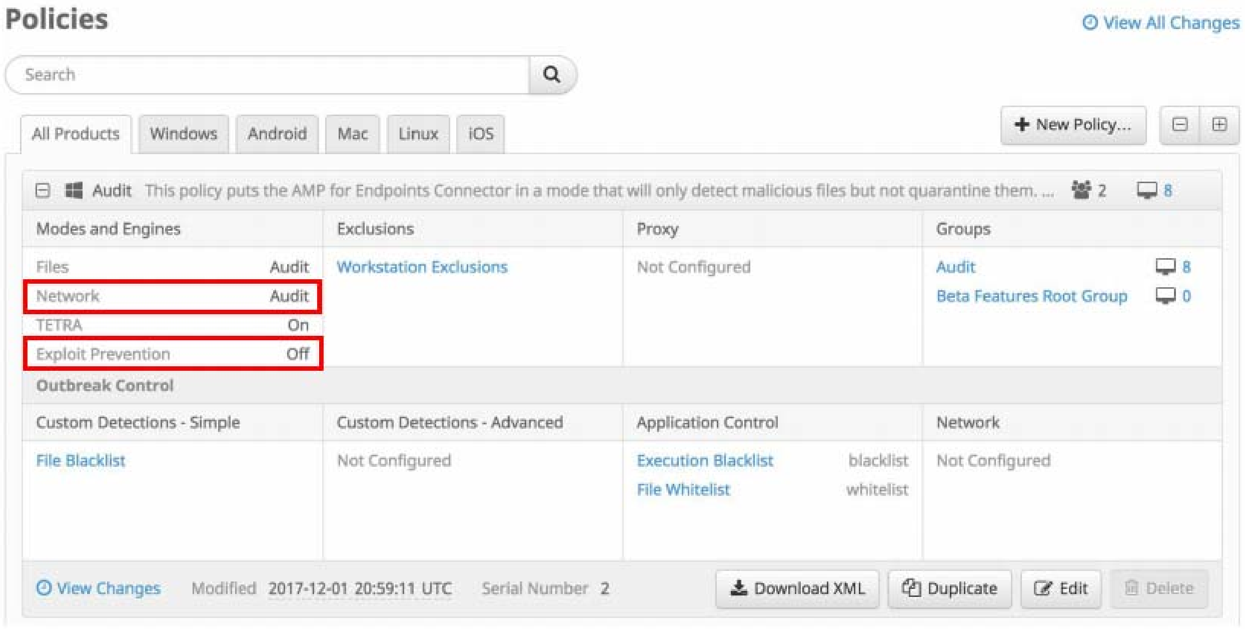
Claim 1 Elements	Applicability
	• Mozilla Firefox 14 or higher • Apple Safari 6 or higher • Google Chrome 20 or higher” Cisco *AMP for Endpoints User Guide*, Chapter 1, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 “**Policy Summary** Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.

Claim 1 Elements	Applicability
	 Policies View All Changes Search All Products Windows Android Mac Linux iOS New Policy... Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 2 8 Modes and Engines: Files Audit; Network Audit; TETRA On; Exploit Prevention Off Exclusions: Workstation Exclusions Proxy: Not Configured Groups: Audit 8; Beta Features Root Group 0 Outbreak Control Custom Detections - Simple: File Blacklist Custom Detections - Advanced: Not Configured Application Control: Execution Blacklist blacklist; File Whitelist whitelist Network: Not Configured View Changes Modified 2017-12-01 20:59:11 UTC Serial Number 2 **View Changes** will take you to a filtered view of the Audit Log showing all the changes for that specific policy. You can also use **View All Changes** at the top of the page to show changes to all policies. Click **Edit** to modify an existing policy or click **Duplicate** if you want to create a new policy with the same settings." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020

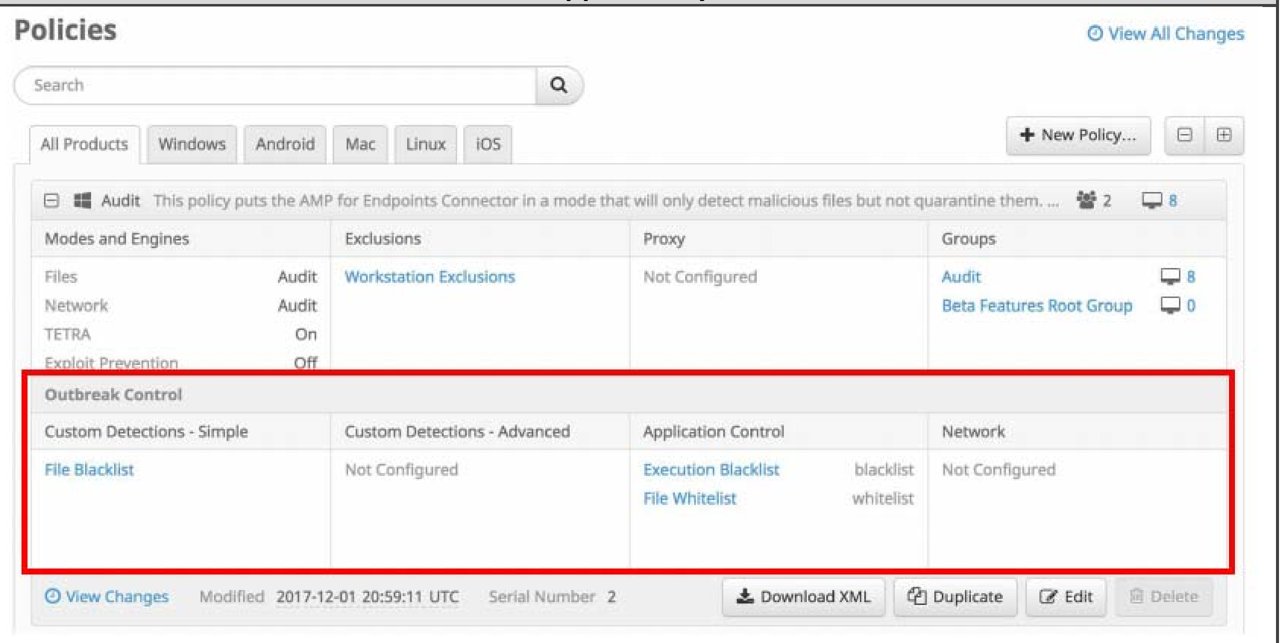
Claim 1 Elements	Applicability
in response to administrator action, causing setting, before the third and fourth events, of a second policy associated with utilizing the traffic inspection-related information that is applied the group including each of the plurality of devices that has the at least one operating system; and	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for, *in response to administrator action* (e.g., user input, etc.)*, causing setting, before the third and fourth events, of a second policy* (e.g., a policy for intrusion-detection software, etc.) *associated with utilizing the traffic inspection-related information* (e.g., signature/policy updates for intrusion-detection software, etc.) *that is applied the group including each of the plurality of devices* (e.g., the 50+ nodes licensed to use the software, etc.) *that has the at least one operating system* (e.g.*,* the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.)*; and* **<u>Note</u>**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): “**Policy Summary** Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.

PRELIMINARY CLAIM CHART

Patent No. 10,873,595, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	 Policies View All Changes Search All Products · Windows · Android · Mac · Linux · iOS New Policy... Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 2 8 Modes and Engines: Files Audit · Network Audit · TETRA On · Exploit Prevention Off Exclusions: Workstation Exclusions Proxy: Not Configured Groups: Audit 8 · Beta Features Root Group 0 Outbreak Control Custom Detections - Simple: File Blacklist Custom Detections - Advanced: Not Configured Application Control: Execution Blacklist blacklist · File Whitelist whitelist Network: Not Configured View Changes Modified 2017-12-01 20:59:11 UTC Serial Number 2 Download XML · Duplicate · Edit · Delete **View Changes** will take you to a filtered view of the Audit Log showing all the changes for that specific policy. You can also use **View All Changes** at the top of the page to show changes to all policies. Click **Edit** to modify an existing policy or click **Duplicate** if you want to create a new policy with the same settings." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020

Claim 1 Elements	Applicability
in response to administrator action, causing setting, before the fifth and sixth events, of a third policy associated with utilizing the firewall-related information that is applied to the group including each of the plurality of devices that has the at least one operating system.	Cisco Advanced Malware Protection (AMP) for Endpoints, when in operation, practices a method for, *in response to administrator action* (e.g., user input, etc.), *causing setting, before the fifth and sixth events, of a third policy* (e.g., a policy for firewall software, etc.) *associated with utilizing the firewall-related information* (e.g., signature/policy updates for firewall software, etc.) *that is applied to the group including each of the plurality of devices* (e.g., the 50+ nodes licensed to use the software, etc.) *that has the at least one operating system* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.). **<u>Note</u>**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "**Policy Summary** Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.

Claim 1 Elements	Applicability
	 Policies View All Changes Search All Products Windows Android Mac Linux iOS New Policy... View Changes Download XML Duplicate Edit Delete Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 2 8 Modes and Engines: Files Audit; Network Audit; TETRA On; Exploit Prevention Off Exclusions: Workstation Exclusions Proxy: Not Configured Groups: Audit 8; Beta Features Root Group 0 Outbreak Control Custom Detections - Simple: File Blacklist Custom Detections - Advanced: Not Configured Application Control: Execution Blacklist blacklist; File Whitelist whitelist Network: Not Configured Modified 2017-12-01 20:59:11 UTC Serial Number 2 **View Changes** will take you to a filtered view of the Audit Log showing all the changes for that specific policy. You can also use **View All Changes** at the top of the page to show changes to all policies. Click **Edit** to modify an existing policy or click **Duplicate** if you want to create a new policy with the same settings." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020

Caveat: The notes and/or cited excerpts utilized herein are set forth for illustrative purposes only and are not meant to be limiting in any manner. For example, the notes and/or cited excerpts, may or may not be supplemented or substituted with different excerpt(s) of the relevant reference(s), as appropriate. Further, to the extent any error(s) and/or omission(s) exist herein, all rights are reserved to correct the same in connection with any subsequent correlations.